

	Project FUSA_BMS_ASIL_C_2W_11_06	09-Jul-2025 1:47 pm
--	--	------------------------

Document Type Functional and Technical Safety Concept

Architecture Technical Architecture

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration or a utility model or design, are reserved.
--

Primary document contact			
Name	Division	Phone	E-Mail

Release Version:				
Date	Name	Function	Division	Signature
		Safety Manager		
		Project Manager		
		Technical Project Manager		
		Quality Manager		

Page	Date	Classification: CONFIDENTIAL	
1 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

Table of Contents

<u>1. Purpose</u>	3
<u>2. Safety goals</u>	4
<u>3. Functional safety requirements</u>	5
<u>4. Technical architecture</u>	9
<u>4.1 2w</u>	9
<u>4.1.1 Element BMS-2W</u>	12
<u>4.2 2W-TA_NEW</u>	12
<u>4.2.1 Element AFEs</u>	15
<u>4.2.2 Element Master Controller</u>	15
<u>4.2.3 Element Power Distribution</u>	15
<u>4.2.4 Element Insulation Monitoring</u>	15
<u>4.2.5 Element Power Supply</u>	15
<u>4.3 TA-2W</u>	15
<u>4.3.1 Element 2W-BMS-ASIL-C</u>	17
<u>5. Safety mechanisms</u>	18
<u>6. Safety requirements</u>	19
<u>6.1. Functional safety requirements</u>	19
<u>6.2. Technical safety requirements</u>	26

Page	Date	Classification: CONFIDENTIAL	
2 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

1 Purpose

This document describes the technical safety concept (TeSiKo) for the FUSA_BMS_ASIL_C_2W_11_06. The TeSiKo defines the technological approach and implementation strategy for the functional safety concept (FuSiKo). It contains all safety goals and shows how the technical safety requirements are realized as safety mechanisms in the system design.

Page	Date	Classification: CONFIDENTIAL	
3 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

2 Safety Goals

This section lists all safety goals that have been considered during the development of the technical safety concept.

ID	Name	Description	Safe state	ASIL
G002	Prevent battery from operating outside SOA	BMS must prevent battery from operating outside its safe operating area at all times	Battery is disconnected when not operating in SOA	C

3 Functional safety requirements

This section outlines the derivation of functional and technical safety requirements and their contribution to safety goals. The following diagrams show the break-down of safety requirements per safety goal. The individual figures have the following meaning:

Icon	Requirement Type
	Safety Goal
	Requirement or Safety Requirement
	Functional Safety Requirement
	Technical Safety Requirement
	Software Safety Requirement
	Hardware Safety Requirement
	Decomposed Safety Requirement

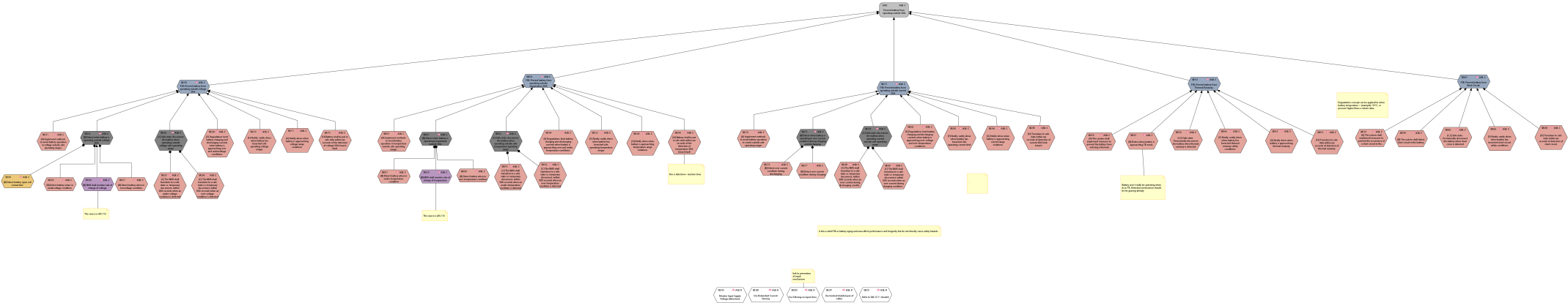


Figure 3.1: FSC Top Level Diagram

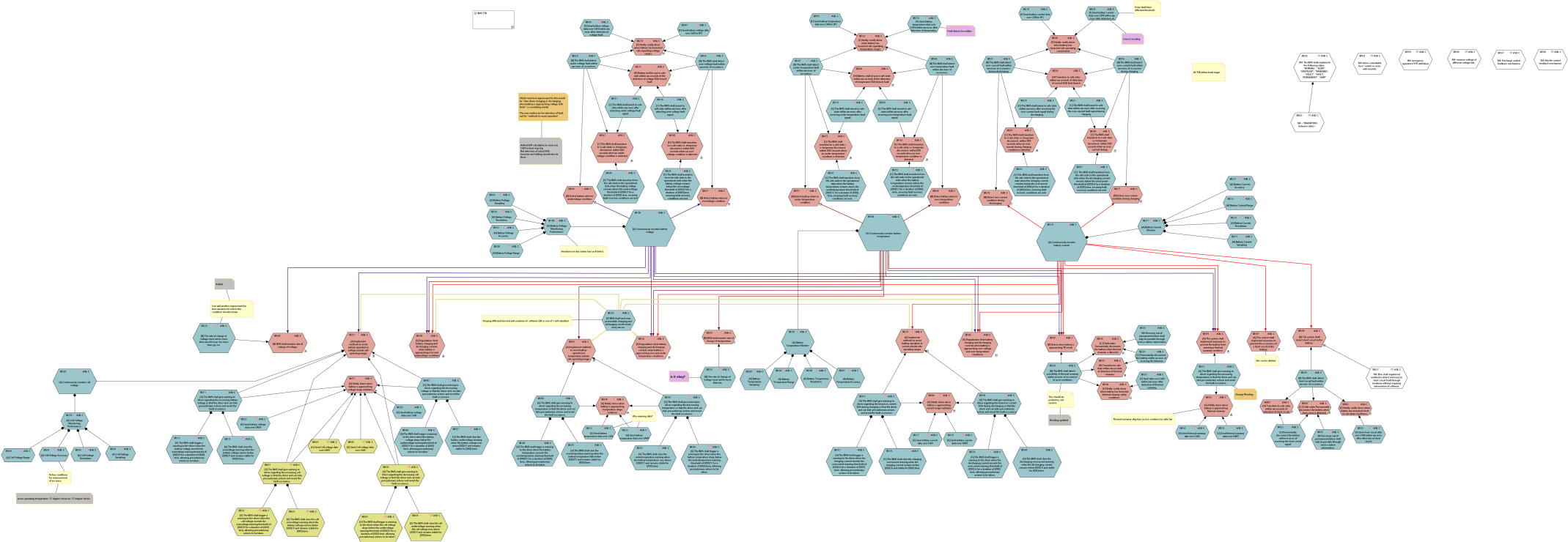


Figure 3.2: Overall TSR



Figure 3.3: BMS TSR

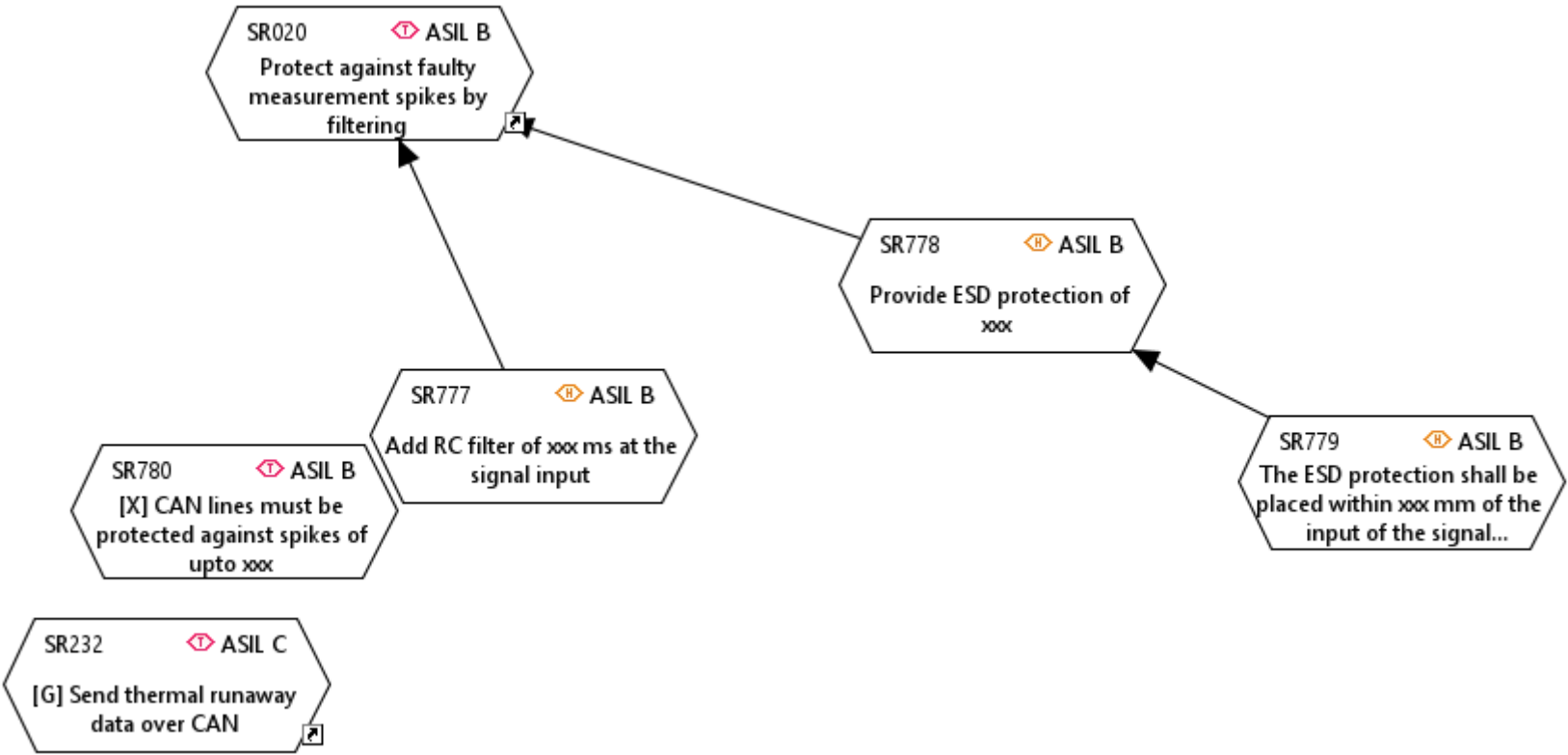


Figure 3.4: HW Safety Concept

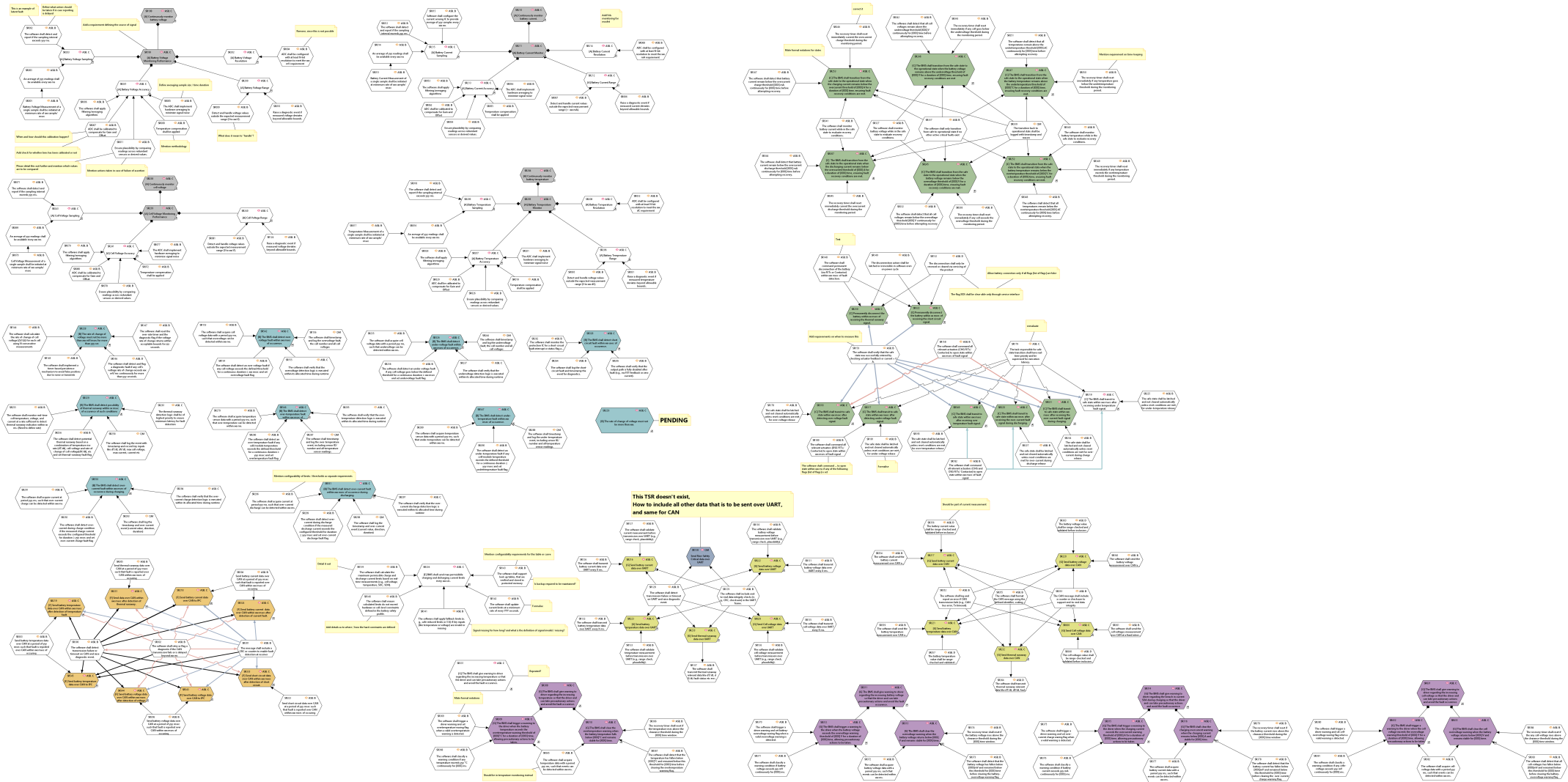


Figure 3.5: SSR_2nd_Iteration

4 Technical Architecture

4.1 2w

Page	Date	Classification: CONFIDENTIAL	
9 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

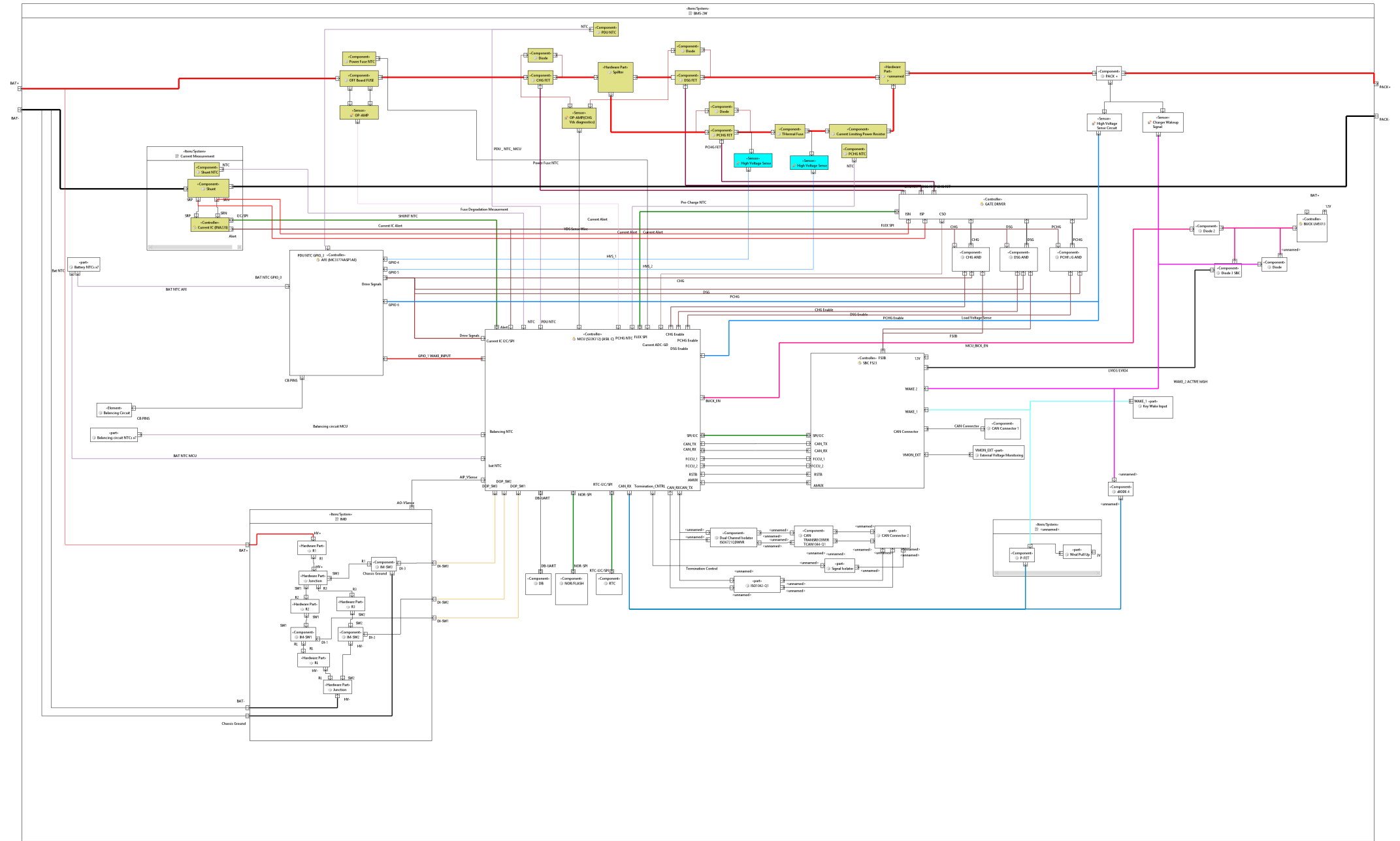


Figure 4.1: 2w

4.1.1 Element BMS-2W

<description missing>

4.2 2W-TA_NEW

Page	Date	Classification: CONFIDENTIAL	
12 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

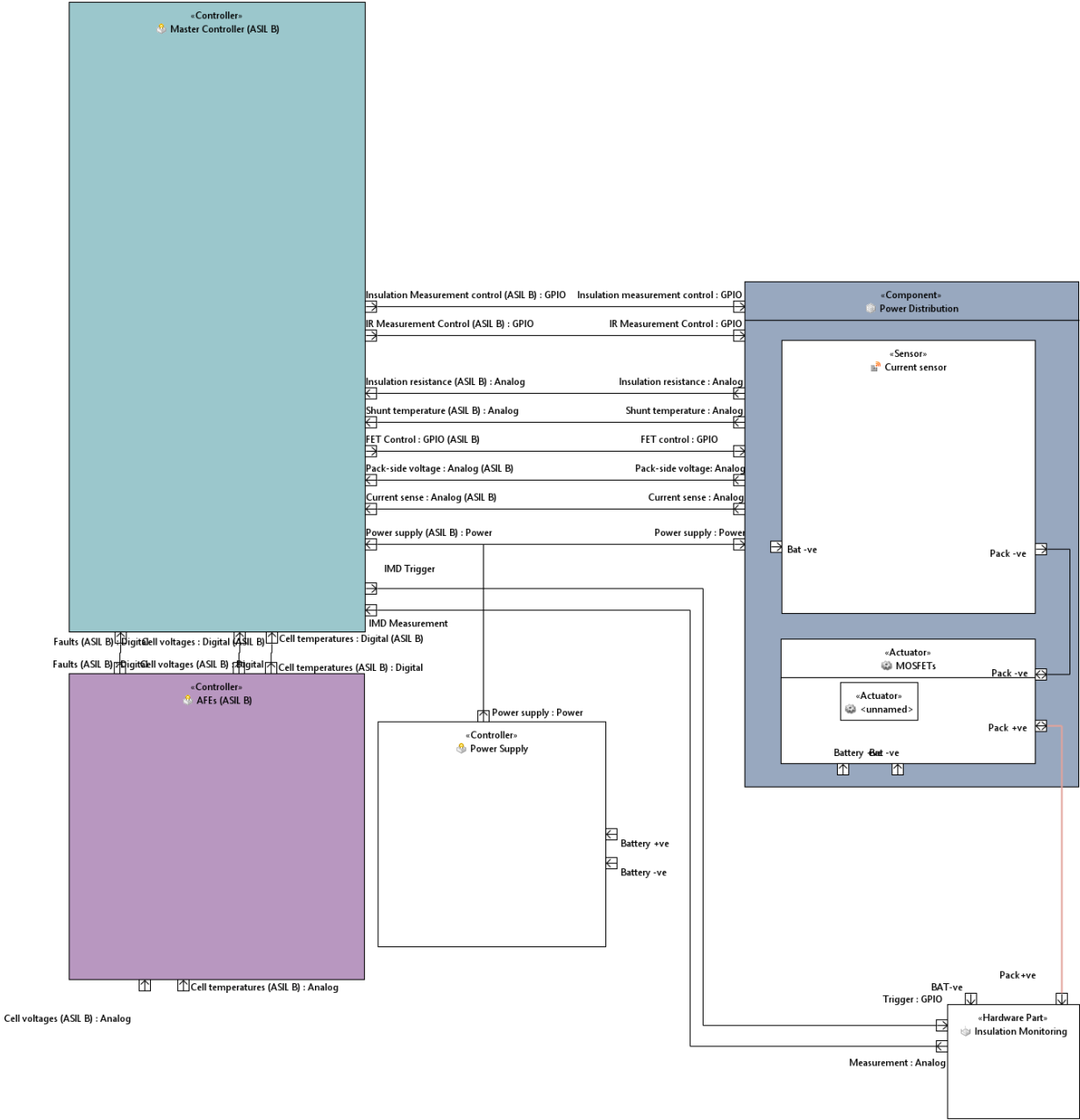


Figure 4.2: 2W-TA_NEW

4.2.1 Element AFEs

<description missing>

4.2.2 Element Master Controller

<description missing>

4.2.3 Element Power Distribution

<description missing>

4.2.4 Element Insulation Monitoring

<description missing>

4.2.5 Element Power Supply

<description missing>

4.3 TA-2W

Page	Date	Classification: CONFIDENTIAL	
15 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

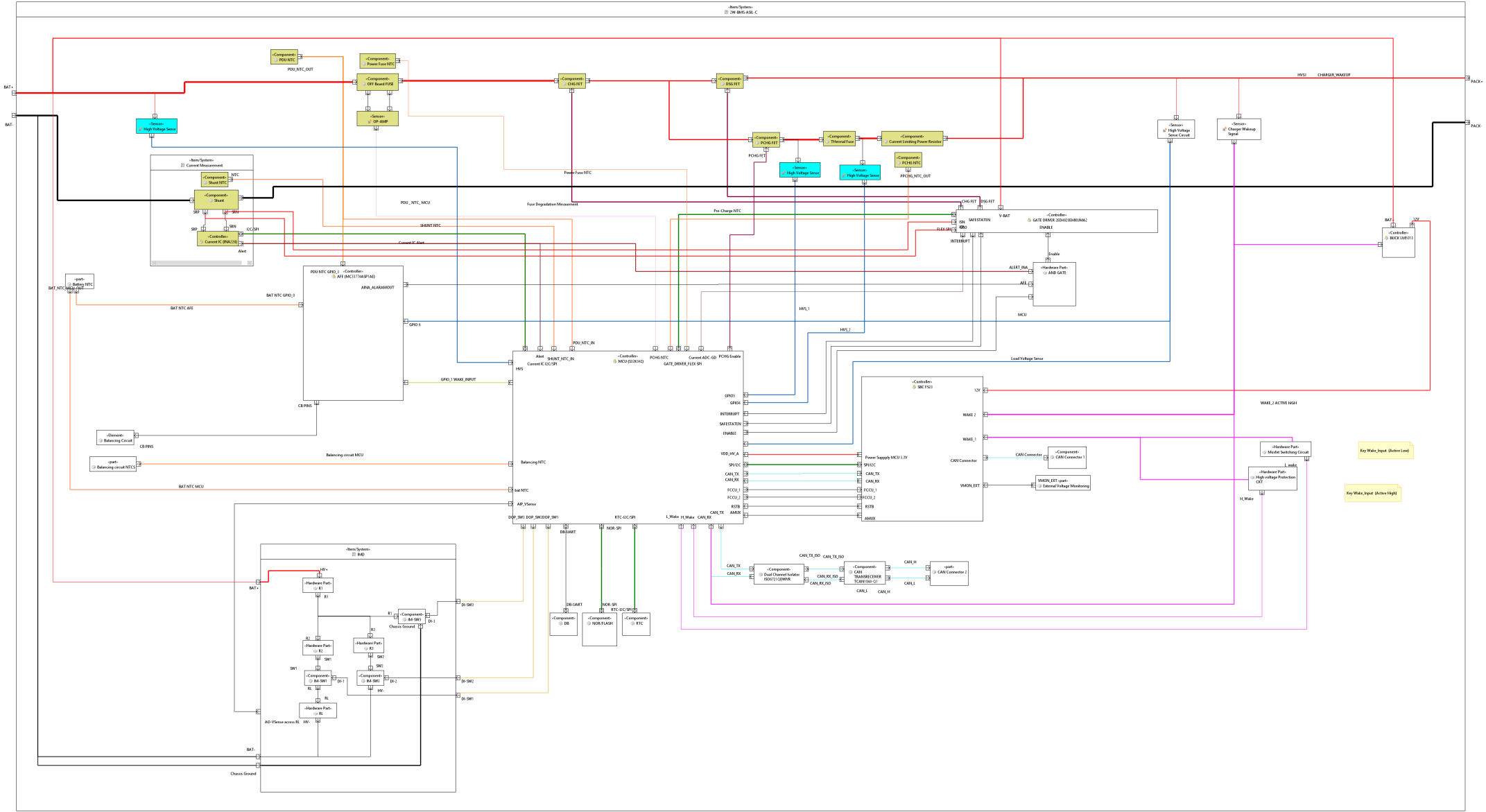


Figure 4.3: TA-2W

4.3.1 Element 2W-BMS-ASIL-C

<description missing>

Page	Date	Classification: CONFIDENTIAL	
17 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

5 Safety mechanisms

Acronym	Safety Mechanism/ Safety Measure	Description	Architecture Elements
	BMS input power short circuit and reverse polarity protection	Implement methods to protect against input short circuit and reverse polarity	
ISO26262-4 D.2.1.1	Failure detection by on-line monitoring		
ISO26262-4 D.2.5.6; D.2.5.7; D.2.5.8	Combination of information redundancy, frame counter and timeout monitoring	End2End Protection	
	Memory Protection Unit	from supplier	

6 Safety requirements

6.1 Functional safety requirements

ID: SR033

FSR: Prevent battery from operating outside temperature SOA (ASIL C)

Allocated to:

Contributes to: G002

ID: SR035

[A] Implement methods to avoid battery operation in temperature outside safe operating ranges (ASIL C)

Allocated to:

Contributes to: G002

ID: SR037

[B] Detect when battery is operating temperature outside SOA (ASIL C)

Allocated to:

Contributes to: G002

ID: SR038

[B] Detect battery when in over-temperature condition (ASIL C)

Allocated to:

Contributes to: G002

ID: SR051

[B] Detect battery when in under-temperature condition (ASIL C)

Allocated to:

Contributes to: G002

ID: SR052

[C] Safe state: disconnect the battery when operating outside safe temperature operating range (ASIL C)

Allocated to:

Contributes to: G002

ID: SR073

[C] The BMS shall transition to a safe state i.e. temporary disconnect, within XXX seconds when an under-temperature condition is detected (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
19 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR102

[C] The BMS shall transition to a safe state i.e. temporary disconnect, within XXX seconds when an over-temperature condition is detected (ASIL C)

Allocated to:

Contributes to: G002

ID: SR104

[E] Degradation: limit battery charging and discharging currents when battery is approaching over and under temperature conditions (ASIL C)

Allocated to:

Contributes to: G002

ID: SR108

IC_BIST_STATUS: BIST_FAILURE_AFE (ASIL B)

Allocated to:

Contributes to:

ID: SR123

[F] Notify: notify driver when battery has breached safe operating temperature ranges (ASIL C)

Allocated to:

Contributes to: G002

ID: SR248

[G] Notify driver when battery is approaching temperature range violations (ASIL C)

Allocated to:

Contributes to: G002

ID: SR249

[H] Battery shall be put in safe state within xxx seconds of the detection of temperature SOA breach fault (ASIL C)

Allocated to:

Contributes to: G002

ID: SR250

FSR: Prevent battery from operating outside voltage SOA (ASIL C)

Allocated to:

Contributes to: G002

ID: SR251

[A] Implement methods to avoid battery operation in voltage outside safe operating ranges (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
20 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR254

[B] Detect when battery is operating outside voltage SOA (ASIL C)

Allocated to:

Contributes to: G002

ID: SR257

[B] Detect battery when in overvoltage condition (ASIL C)

Allocated to:

Contributes to: G002

ID: SR260

[B] Detect battery when in undervoltage condition (ASIL C)

Allocated to:

Contributes to: G002

ID: SR263

[C] Safe state: disconnect the battery when operating outside voltage safe operating range (ASIL C)

Allocated to:

Contributes to: G002

ID: SR267

[C] The BMS shall transition to a safe state i.e. temporary disconnect, within XXX seconds when an under-voltage condition is detected (ASIL C)

Allocated to:

Contributes to: G002

ID: SR268

[C] The BMS shall transition to a safe state i.e. temporary disconnect, within XXX seconds when an over-voltage condition is detected (ASIL C)

Allocated to:

Contributes to: G002

ID: SR269

[E] Degradation: limit battery charging and discharging currents when battery is approaching over and undervoltage conditions (ASIL C)

Allocated to:

Contributes to: G002

ID: SR270

[F] Notify: notify driver when battery has breached safe operating voltage ranges (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
21 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR271

[G] Notify driver when battery is approaching voltage range violations (ASIL C)

Allocated to:

Contributes to: G002

ID: SR272

[H] Battery shall be put in safe state within xxx seconds of the detection of voltage SOA breach fault (ASIL C)

Allocated to:

Contributes to: G002

ID: SR273

FSR: Prevent battery from operating outside current SOA (ASIL C)

Allocated to:

Contributes to: G002

ID: SR274

[A] Implement methods to avoid battery operation in current outside safe operating ranges (ASIL C)

Allocated to:

Contributes to: G002

ID: SR275

[B] Detect when battery is operating in over current condition during charging and discharging (ASIL C)

Allocated to:

Contributes to: G002

ID: SR276

[B] Detect over current condition during discharging (ASIL C)

Allocated to:

Contributes to: G002

ID: SR277

[B] Detect over current condition during charging (ASIL C)

Allocated to:

Contributes to: G002

ID: SR278

[C] Safe state: disconnect the battery when operating current outside safe operating range (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
22 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR280

[C] The BMS shall transition to a safe state i.e. temporary disconnect, within XXX seconds when an over-current during discharging condition is detected (ASIL C)

Allocated to:

Contributes to: G002

ID: SR281

[C] The BMS shall transition to a safe state i.e. temporary disconnect, within XXX seconds when an over-current during charging condition is detected (ASIL C)

Allocated to:

Contributes to: G002

ID: SR282

[E] Degradation: limit battery charging and discharging currents when battery is approaching over-voltage and over-temperature conditions (ASIL C)

Allocated to:

Contributes to: G002

ID: SR283

[F] Notify: notify driver when battery has breached safe operating current limit (ASIL C)

Allocated to:

Contributes to: G002

ID: SR284

[G] Notify driver when battery is approaching current range violations (ASIL C)

Allocated to:

Contributes to: G002

ID: SR285

[H] Transition to safe state within xxx seconds of detection of current SOA limit breach (ASIL C)

Allocated to:

Contributes to: G002

ID: SR330

[B] BMS shall monitor rate of change of temperature. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR387

Use twisted/shielded pair of cables (ASIL D)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
23 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR388
Use Redundant Current Sensing (ASIL D)
Allocated to:
Contributes to:

ID: SR389
Use Filtering on input Lines (ASIL D)
Allocated to:
Contributes to:

ID: SR390
Monitor Input Supply Voltage [detection] (ASIL D)
Allocated to:
Contributes to:

ID: SR391
Refer to SAE J2111 standard (ASIL D)
Allocated to:
Contributes to:

ID: SR548
[B] BMS shall monitor rate of change of voltage. (ASIL C)
Allocated to:
Contributes to: G002

ID: SR552
[H] Transition to safe state within xxx seconds of detection of thermal runaway (ASIL C)
Allocated to:
Contributes to: G002

ID: SR553
FSR: Prevent battery from Thermal Runaway. (ASIL C)
Allocated to:
Contributes to: G002

ID: SR555
[G] Notify driver when battery is approaching thermal runaway (ASIL C)
Allocated to:
Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
24 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR556

[C,E] Safe state: Permanently disconnect the battery when thermal runaway is detected (ASIL C)

Allocated to:

Contributes to: G002

ID: SR559

[A] The system shall implement measures to prevent the battery from entering a thermal runaway condition. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR561

[B] Detect when battery is approaching TR event. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR564

[F] Notify: notify driver when battery has breached thermal runaway safety conditions. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR597

[A] The system shall implement measures to prevent the occurrence of a short circuit in the battery. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR599

[B] The system shall detect short circuit in the battery. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR600

[H] Transition to safe state within xxx seconds of detection of short circuit (ASIL C)

Allocated to:

Contributes to: G002

ID: SR601

FSR: Prevent battery from Short Circuit. (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
25 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR602

[F] Notify: notify driver when battery has breached short circuit safety conditions. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR603

[C,E] Safe state: Permanently disconnect the battery when short circuit is detected (ASIL C)

Allocated to:

Contributes to: G002

ID: SR781

[B] Detect battery open cell connection (ASIL C)

Allocated to:

Contributes to: G002

6.2 Technical safety requirements

ID: SR020

Protect against faulty measurement spikes by filtering (ASIL B)

Allocated to:

Contributes to:

ID: SR022

Filter measurement (ASIL B)

Allocated to:

Contributes to:

ID: SR023

Temporary disconnect the battery if overtemperature has been detected in BMS (ASIL B)

Allocated to:

Contributes to:

ID: SR024

Close switches at IC_TEMP_STATUS: NORMAL (ASIL B)

Allocated to:

Contributes to:

ID: SR025

Open switches at IC_TEMP_STATUS: FAILURE (ASIL B)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
26 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR027

Notify driver and passengers about fault and warning condition of the HV Switch (ASIL B)

Allocated to:

Contributes to:

ID: SR034

HV_SWITCH_STATUS: FAILURE (ASIL B)

Allocated to:

Contributes to:

ID: SR036

HV_SWITCH_STATUS: NORMAL (ASIL B)

Allocated to:

Contributes to:

ID: SR039

Protect BMS from undesired effects of uncontrolled uC power-down (ASIL B)

Allocated to:

Contributes to:

ID: SR040

Brownout (ASIL B)

Allocated to:

Contributes to:

ID: SR041

Notify the driver and passengers about BMS overtemperature (ASIL B)

Allocated to:

Contributes to:

ID: SR042

Permanently disconnect the battery if Mosfets/Contactor is faulty (ASIL B)

Allocated to:

Contributes to:

ID: SR043

SM: Recovery out of permanent failure shall only be possible through service station intervention.
(ASIL B)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
27 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR044

Continuously monitor BMS internal temperatures (ASIL B)

Allocated to:

Contributes to:

ID: SR045

IC die temperature measurements (ASIL B)

Allocated to:

Contributes to:

ID: SR046

Make BMS enter fault state in case of either of MCU, AFE, or SBC reaching high die temperature (ASIL B)

Allocated to:

Contributes to:

ID: SR047

Recover BMS from fault state to normal state when temperatures are within permissible operating range for each part on the BMS (ASIL B)

Allocated to:

Contributes to:

ID: SR048

Shunt temperature measurement performance (ASIL B)

Allocated to:

Contributes to:

ID: SR049

HV Switch temperature measurement performance (ASIL B)

Allocated to:

Contributes to:

ID: SR050

Perform BIST (ASIL B)

Allocated to: MCU (S32K342)

Contributes to:

ID: SR057

IC self test (ASIL B)

Allocated to: MCU (S32K342)

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
28 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR058
Continuously monitor HV FETs voltages (ASIL B)
Allocated to:
Contributes to:

ID: SR059
HV voltage measurement performance (ASIL B)
Allocated to:
Contributes to:

ID: SR060
HV Switch failure detection algorithm (ASIL B)
Allocated to:
Contributes to:

ID: SR061
Detect HV switch failure in short (ASIL B)
Allocated to:
Contributes to:

ID: SR063
Detect HV switch failure in open (ASIL B)
Allocated to:
Contributes to:

ID: SR064
Temporary disconnect the battery if external communication errors have been detected in BMS (ASIL B)
Allocated to:
Contributes to:

ID: SR065
Close switches at EXT_COM_STATUS: NORMAL (ASIL B)
Allocated to:
Contributes to:

ID: SR074
Close switches at EXT_COM_STATUS: WARNING or NORMAL (ASIL B)
Allocated to:
Contributes to:

Page	Date	Classification: CONFIDENTIAL	
29 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR075

Open switches at EXT_COM_STATUS: TIMEOUT (ASIL B)

Allocated to:

Contributes to:

ID: SR076

Open switches at EXT_COM_STATUS: FAILURE (ASIL B)

Allocated to:

Contributes to:

ID: SR082

Protect BMS from hanging (ASIL B)

Allocated to:

Contributes to:

ID: SR083

Watchdog (ASIL B)

Allocated to:

Contributes to:

ID: SR084

Temporary disconnect the battery if bit-flip has been detected in memory (ASIL B)

Allocated to:

Contributes to:

ID: SR085

Close switches at MEMORY_STATUS: WARN or NORMAL (ASIL B)

Allocated to:

Contributes to:

ID: SR086

Open switches at MEMORY_STATUS: FAILURE (ASIL B)

Allocated to:

Contributes to:

ID: SR087

Notify the driver and passengers about BMS external communication error (ASIL B)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
30 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR088
- EXT_COM_FAILURE_TIMEOUT - COMS_STATUS: TIMEOUT (ASIL B)
Allocated to:
Contributes to:

ID: SR089
EXT_COM_STATUS: NORMAL (ASIL B)
Allocated to:
Contributes to:

ID: SR090
EXT_COM_STATUS: EXT_COM_WARN (ASIL B)
Allocated to:
Contributes to:

ID: SR091
EXT_COM_STATUS: EXT_COM_FAILURE (ASIL B)
Allocated to:
Contributes to:

ID: SR092
Notify driver and passengers about internal memory errors (ASIL B)
Allocated to:
Contributes to:

ID: SR093
MEMORY_STATUS: MEMORY_ECC_FAILURE (ASIL B)
Allocated to:
Contributes to:

ID: SR094
MEMORY_STATUS: MEMORY_ECC_WARN (ASIL B)
Allocated to:
Contributes to:

ID: SR095
MEMORY_STATUS: NORMAL (ASIL B)
Allocated to:
Contributes to:

Page	Date	Classification: CONFIDENTIAL	
31 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR096
Continuously monitor BMS external communications (ASIL B)
Allocated to:
Contributes to:

ID: SR097
EDC on external communication (ASIL B)
Allocated to:
Contributes to:

ID: SR098
CRC on external communication (ASIL B)
Allocated to:
Contributes to:

ID: SR099
Periodic external communication timers (ASIL B)
Allocated to:
Contributes to:

ID: SR100
Implement ECC in all memories (ASIL B)
Allocated to:
Contributes to:

ID: SR101
ECC memory (ASIL B)
Allocated to:
Contributes to:

ID: SR103
Notify driver and passengers about BIST detected failure (ASIL B)
Allocated to:
Contributes to:

ID: SR105
IC_BIST_STATUS: BIST_FAILURE_SBC (ASIL B)
Allocated to:
Contributes to:

Page	Date	Classification: CONFIDENTIAL	
32 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR106
IC_BIST_STATUS: BIST_FAILURE_MCU (ASIL B)
Allocated to:
Contributes to:

ID: SR107
IC_BIST_STATUS: BIST_FAILURE_BJB (ASIL B)
Allocated to:
Contributes to:

ID: SR109
IC_BIST_STATUS: NORMAL (ASIL B)
Allocated to:
Contributes to:

ID: SR110
Temporary disconnect the battery if BIST detected failure in BMS (ASIL B)
Allocated to:
Contributes to:

ID: SR111
Close switches at IC_BIST_STATUS: NORMAL (ASIL B)
Allocated to:
Contributes to:

ID: SR112
Open switches at IC_BIST_STATUS: FAILURE (ASIL B)
Allocated to:
Contributes to:

ID: SR113
Provide BMS with absolute time (ASIL B)
Allocated to:
Contributes to:

ID: SR114
Absolute time life (ASIL B)
Allocated to:
Contributes to:

Page	Date	Classification: CONFIDENTIAL	
33 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR115
Absolute time resolution (ASIL B)
Allocated to:
Contributes to:

ID: SR116
Provide BMS counter for timestamped Reset events (ASIL B)
Allocated to:
Contributes to:

ID: SR117
Store RESET Count in NV memory (ASIL B)
Allocated to:
Contributes to:

ID: SR118
Access RESET Count (ASIL B)
Allocated to:
Contributes to:

ID: SR119
Maintain proper operation at re-boot (ASIL B)
Allocated to:
Contributes to:

ID: SR120
Store configuration & Flags (ASIL B)
Allocated to:
Contributes to:

ID: SR121
Retrieve configuration & Flags at boot (ASIL B)
Allocated to:
Contributes to:

ID: SR122
Program configuration & Flags (ASIL B)
Allocated to:
Contributes to:

Page	Date	Classification: CONFIDENTIAL	
34 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR134

Continuously monitor BMS internal communications (ASIL B)

Allocated to:

Contributes to:

ID: SR138

Send Non-Safety Critical data over UART (ASIL QM)

Allocated to:

Contributes to:

ID: SR157

CRC on internal communication (ASIL B)

Allocated to:

Contributes to:

ID: SR160

EDC on internal communication (ASIL B)

Allocated to:

Contributes to:

ID: SR161

Periodic external communication timers (ASIL B)

Allocated to:

Contributes to:

ID: SR162

Periodic internal communication timers (ASIL B)

Allocated to:

Contributes to:

ID: SR163

Retry communication (ASIL B)

Allocated to:

Contributes to:

ID: SR164

The BMS shall raise flag COMM ERROR in case of continued failure (ASIL B)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
35 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR165

Notify the driver and passengers about BMS internal communication error (ASIL B)

Allocated to:

Contributes to:

ID: SR166

Temporary disconnect the battery if internal communication is faulty (ASIL B)

Allocated to:

Contributes to:

ID: SR167

Open switches at INT_COM_STATUS: TIMEOUT (ASIL B)

Allocated to:

Contributes to:

ID: SR168

Close switches at INT_COM_STATUS: NORMAL (ASIL B)

Allocated to:

Contributes to:

ID: SR169

Open switches at COM_STATUS: FAILURE (ASIL B)

Allocated to:

Contributes to:

ID: SR170

Close switches at COM_STATUS: WARNING or NORMAL (ASIL B)

Allocated to:

Contributes to:

ID: SR171

Protect against SW errors by use of adequate SW design approach (ASIL B)

Allocated to:

Contributes to:

ID: SR172

Use of 2-level software architecture (ASIL B)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
36 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR173

The BMS shall receive external commands and send external information over CAN (ASIL B)

Allocated to:

Contributes to:

ID: SR174

Flags over CAN (ASIL B)

Allocated to:

Contributes to:

ID: SR175

E2E protected CAN (ASIL B)

Allocated to:

Contributes to:

ID: SR176

Open HV switch (ASIL B)

Allocated to:

Contributes to:

ID: SR177

Permanent Flag (ASIL B)

Allocated to:

Contributes to:

ID: SR185

Close HV switch (ASIL B)

Allocated to:

Contributes to:

ID: SR186

Prevent BMS failures related to production quality (ASIL B)

Allocated to:

Contributes to:

ID: SR187

PCB manufacturing (ASIL B)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
37 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR188

The BMS shall keep track and act upon internal and external events (ASIL B)

Allocated to:

Contributes to:

ID: SR189

Flags (ASIL B)

Allocated to:

Contributes to:

ID: SR190

The BMS shall provide means of measurement calibration (ASIL B)

Allocated to:

Contributes to:

ID: SR191

Store calibration (ASIL B)

Allocated to:

Contributes to:

ID: SR192

Retrieve configuration & Flags at boot (ASIL B)

Allocated to:

Contributes to:

ID: SR193

Program configuration & Flags (ASIL B)

Allocated to:

Contributes to:

ID: SR194

Provide protections for internal voltage faults (ASIL B)

Allocated to:

Contributes to:

ID: SR196

Open switches at HV_SWITCH_STATUS: FAILURE (ASIL B)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
38 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR197

Close switches at HV_SWITCH_STATUS: NORMAL (ASIL B)

Allocated to:

Contributes to:

ID: SR198

[A] Continuously monitor battery voltage (ASIL C)

Allocated to:

Contributes to: G002

ID: SR199

[A] Battery Voltage Monitoring Performance (ASIL C)

Allocated to:

Contributes to: G002

ID: SR200

[A] Battery Voltage Range (ASIL C)

Allocated to:

Contributes to: G002

ID: SR201

[A] Battery Voltage Accuracy (ASIL C)

Allocated to:

Contributes to: G002

ID: SR202

[A] Battery Voltage Resolution (ASIL C)

Allocated to:

Contributes to: G002

ID: SR203

[A] Battery Voltage Sampling (ASIL C)

Allocated to:

Contributes to: G002

ID: SR204

[A] Continuously monitor battery temperature (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
39 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR205
[A] Battery Temperature Monitor (ASIL C)
Allocated to:
Contributes to: G002

ID: SR206
[A] Battery Temperature Range (ASIL C)
Allocated to:
Contributes to: G002

ID: SR207
[A] Battery Temperature Accuracy (ASIL C)
Allocated to:
Contributes to: G002

ID: SR208
[A] Battery Temperature Resolution (ASIL C)
Allocated to:
Contributes to: G002

ID: SR209
[A] Battery Temperature Sampling (ASIL C)
Allocated to:
Contributes to: G002

ID: SR210
[A] Continuously monitor battery current. (ASIL C)
Allocated to:
Contributes to: G002

ID: SR211
[A] Battery Current Monitor (ASIL C)
Allocated to:
Contributes to: G002

ID: SR212
[A] Battery Current Range (ASIL C)
Allocated to:
Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
40 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR213
[A] Battery Current Accuracy (ASIL C)
Allocated to:
Contributes to: G002

ID: SR214
[A] Battery Current Resolution (ASIL C)
Allocated to:
Contributes to: G002

ID: SR215
[A] Battery Current Sampling (ASIL C)
Allocated to:
Contributes to: G002

ID: SR216
[G] Send battery current data over UART (ASIL C)
Allocated to:
Contributes to: G002

ID: SR217
[G] Send battery current data over CAN (ASIL C)
Allocated to:
Contributes to: G002

ID: SR218
[F] Send battery current data over CAN to IPC (ASIL C)
Allocated to:
Contributes to: G002

ID: SR219
[F] Send battery temperature data over CAN within xxx msec after detection of temperature fault.
(ASIL C)
Allocated to:
Contributes to: G002

ID: SR220
[G] Send battery voltage data over CAN (ASIL C)
Allocated to:
Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
41 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR221
[G] Send battery temperature data over CAN (ASIL C)
Allocated to:
Contributes to: G002

ID: SR222
[G] Send battery voltage data over UART (ASIL C)
Allocated to:
Contributes to: G002

ID: SR223
[G] Send battery temperature data over UART (ASIL C)
Allocated to:
Contributes to: G002

ID: SR226
[E] BMS shall send max permissible charging and discharging current limits every xxx sec. (ASIL C)
Allocated to:
Contributes to: G002

ID: SR228
[B] The rate of change of voltage must not be more than xxx mV/msec for more than yyy sec (ASIL C)
Allocated to:
Contributes to: G002

ID: SR229
[B] The rate of change of voltage must not be more than xxx. (ASIL C)
Allocated to:
Contributes to: G002

ID: SR230
[C] Permanently disconnect the battery within xx msec of receiving the thermal runaway signal. (ASIL C)
Allocated to:
Contributes to: G002

ID: SR231
[F] Send data over CAN within xxx msec after detection of thermal runaway. (ASIL C)
Allocated to:
Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
42 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR232
[G] Send thermal runaway data over CAN (ASIL C)
Allocated to:
Contributes to: G002

ID: SR233
[G] Send thermal runaway data over UART (ASIL C)
Allocated to:
Contributes to: G002

ID: SR238
[A] Continuously monitor cell voltage (ASIL C)
Allocated to:
Contributes to: G002

ID: SR239
[A] Cell Voltage Monitoring Performance (ASIL C)
Allocated to:
Contributes to: G002

ID: SR240
[A] Cell Voltage Range (ASIL C)
Allocated to:
Contributes to: G002

ID: SR241
[A] Cell Voltage Accuracy (ASIL C)
Allocated to:
Contributes to: G002

ID: SR242
[A] Cell Voltage Resolution (ASIL C)
Allocated to:
Contributes to: G002

ID: SR243
[A] Cell Voltage Sampling (ASIL C)
Allocated to:
Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
43 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR245

[C] The BMS shall transition from the safe state to the operational state when the battery voltage remains below the overvoltage threshold of [XXX] V for a duration of [XXX] time, ensuring fault recovery conditions are met. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR246

[C] The BMS shall transition from the safe state to the operational state when the battery voltage remains above the undervoltage threshold of [XXX] V for a duration of [XXX] time, ensuring fault recovery conditions are met (ASIL C)

Allocated to:

Contributes to: G002

ID: SR247

[C] The BMS shall transition from the safe state to the operational state when the battery temperature remains above the undertemperature threshold of [XXX]°C for a duration of [XXX] time, ensuring fault recovery conditions are met. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR252

[C] The BMS shall transition from the safe state to the operational state when the battery temperature remains below the overtemperature threshold of [XXX]°C for a duration of [XXX] time, ensuring fault recovery conditions are met. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR253

[C] The BMS shall transition from the safe state to the operational state when the charging current remains below the overcurrent threshold of [XXX] A for a duration of [XXX] time, ensuring fault recovery conditions are met. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR307

[C] The BMS shall transition from the safe state to the operational state when the discharging current remains below the overcurrent threshold of [XXX] A for a duration of [XXX] time, ensuring fault recovery conditions are met. (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
44 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR308

[G] The BMS shall give warning to driver regarding the increasing temperature so that the driver and can take precautionary actions and avoid the fault occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR309

[G] The BMS shall trigger a warning to the driver when the battery temperature exceeds the overtemperature warning threshold of [XXX]°C for a duration of [XXX] time, allowing precautionary actions to be taken. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR310

[G] The BMS shall clear the overtemperature warning when the battery temperature falls below [XXX] °C and remains stable for [XXX] time. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR311

[G] The BMS shall give warning to driver regarding the increasing battery voltage so that the driver and can take precautionary actions and avoid the fault occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR312

[G] The BMS shall trigger a warning to the driver when the battery voltage exceeds the overvoltage warning threshold of [XXX] V for a duration of [XXX] time, allowing precautionary actions to be taken. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR313

[G] The BMS shall clear the overvoltage warning when the battery voltage returns below [XXX] V and remains stable for [XXX] time. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR314

[G] The BMS shall give warning to driver regarding the breach in current SOA during charging so that the driver and can take precautionary actions and avoid the fault occurrence. (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
45 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR315

[G] The BMS shall trigger a warning to the driver when the charging current exceeds the overcurrent warning threshold of [XXX] A for a duration of [XXX] time, allowing precautionary actions to be taken.

(ASIL C)

Allocated to:

Contributes to: G002

ID: SR316

[G] The BMS shall clear the charging overcurrent warning when the charging current remains below [XXX] A and stable for [XXX] time. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR317

[C] The BMS shall transit to safe state within xxx msec after detecting under voltage fault signal.

(ASIL C)

Allocated to:

Contributes to: G002

ID: SR318

[C] The BMS shall transit to safe state within xxx msec after detecting over voltage fault signal. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR319

[C] The BMS shall transit to safe state within xxx msec after receiving under temperature fault signal.

(ASIL C)

Allocated to:

Contributes to: G002

ID: SR320

[C] The BMS shall transit to safe state within xxx msec after receiving the over-current fault signal during discharging. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR321

[C] The BMS shall transit to safe state within xxx msec after receiving the over-current fault signal during charging. (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
46 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR322

[C] Permanently disconnect the battery within xx msec of receiving the short circuit signal. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR324

[F] Send battery current data over CAN within xxx msec after detection of current fault. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR325

SM: Recovery out of permanent failure shall only be possible through service station intervention. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR326

[B] The BMS shall detect under-voltage fault within xxx msec of occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR328

[B] The BMS shall detect short circuit fault within xxx usec of occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR329

[B] The BMS shall detect possibility of thermal runaway within xx msec of occurrence of such conditions (ASIL C)

Allocated to:

Contributes to: G002

ID: SR331

[G] The BMS shall give warning to driver regarding the increasing temperature so that the driver and can take precautionary actions and avoid the fault occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR333

[F] Send short circuit data over CAN within xxx msec after detection of short circuit. (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
47 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR334

[G] The BMS shall give warning to driver regarding the deacreasing temperature so that the driver and can take precautionary actions and avoid the fault occurence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR335

[G] The BMS shall clear the undertemperature warning when the battery temperature rises above [XXX]°C and remains stable for [XXX] time. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR336

[G] The BMS shall trigger a warning to the driver when the battery temperature drops below the undertemperature warning threshold of [XXX]°C for a duration of [XXX] time, allowing precautionary actions to be taken. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR445

[G] The BMS shall give warning to driver regarding the decreasing voltage so that the driver and can take precautionary actions and avoid the fault occurence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR446

[G] The BMS shall trigger a warning to the driver when the battery voltage drops below the undervoltage warning threshold of [XXX] V for a duration of [XXX] time, allowing precautionary actions to be taken." (ASIL C)

Allocated to:

Contributes to: G002

ID: SR537

[G] The BMS shall clear the battery undervoltage warning when the battery voltage rises above [XXX] V and remains stable for [XXX] time. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR538

[G] The BMS shall give warning to driver regarding the breach in current SOA during discharging so that the driver and can take precautionary actions and avoid the fault occurence. (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
48 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR539

[G] The BMS shall trigger a warning to the driver when the discharging current exceeds the overcurrent warning threshold of [XXX] A for a duration of [XXX] time, allowing precautionary actions to be taken. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR540

[G] The BMS shall clear the discharging overcurrent warning when the discharging current remains below [XXX] A and stable for [XXX] time. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR541

SM: Recovery out of permanent failure shall only be possible through service station intervention. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR542

[B] The BMS shall detect over-voltage fault within xxx msec of occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR543

[F] Send battery voltage data over CAN to IPC (ASIL C)

Allocated to:

Contributes to: G002

ID: SR544

[F] Send battery voltage data over CAN within xxx msec after detection of voltage fault. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR545

[F] Send battery temperature data over CAN to IPC (ASIL C)

Allocated to:

Contributes to: G002

ID: SR546

[B] The BMS shall detect over-temperature fault within xxx msec of occurrence. (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
49 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR547

[B] The BMS shall detect under-temperature fault within xxx msec of occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR549

[C] The BMS shall transit to safe state within xxx msec after receiving over temperature fault signal. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR550

[B] The BMS shall detect over-current fault within xxx msec of occurrence during charging. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR551

[B] The BMS shall detect over-current fault within xxx msec of occurrence during discharging. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR557

SM: Bms shall implement method to detect and react to short circuit fault through hardware without requiring intervention of software. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR562

SM: The BMS shall implement the following states: "NORMAL", "SLEEP", "DEEPSLEEP", "WARNING", "FAULT". "FAULT_PERMANENT", "LIMP" (ASIL C)

Allocated to:

Contributes to:

ID: SR563

SM: (ASIL C)

Allocated to:

Contributes to:

ID: SR565

SM: Inline controllable fuse / switch in series with mosfets (ASIL C)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
50 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR566
SM: Mosfet control feedback mechanism (ASIL C)
Allocated to:
Contributes to:

ID: SR567
SM: Precharge control feedback mechanism (ASIL C)
Allocated to:
Contributes to:

ID: SR568
SM: measure voltage of different voltage rails (ASIL C)
Allocated to:
Contributes to:

ID: SR569
SM: emergency operation FHTI definition (ASIL C)
Allocated to:
Contributes to:

ID: SR571
Boot Loader (ASIL D)
Allocated to:
Contributes to:

ID: SR573
cyber security (ASIL D)
Allocated to:
Contributes to:

ID: SR575
Access control (ASIL D)
Allocated to:
Contributes to:

ID: SR576
Reliability requirement: signal connectors (ASIL D)
Allocated to:
Contributes to:

Page	Date	Classification: CONFIDENTIAL	
51 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR629

[G] Send Cell voltage data over UART (ASIL C)

Allocated to:

Contributes to: G002

ID: SR630

[G] Send Cell voltage data over CAN (ASIL C)

Allocated to:

Contributes to: G002

ID: SR631

[G] The BMS shall give warning to driver regarding the increasing cell voltage so that the driver and can take precautionary actions and avoid the fault occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR632

[G] The BMS shall trigger a warning to the driver when the cell voltage exceeds the overvoltage warning threshold of [XXX] V for a duration of [XXX] time, allowing precautionary actions to be taken. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR633

[G] The BMS shall clear the cell overvoltage warning when the battery voltage returns below [XXX] V and remains stable for [XXX] time. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR634

[G] The BMS shall give warning to driver regarding the decreasing cell voltage so that the driver and can take precautionary actions and avoid the fault occurrence. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR635

[G] The BMS shall trigger a warning to the driver when the cell voltage drops below the undervoltage warning threshold of [XXX] V for a duration of [XXX] time, allowing precautionary actions to be taken." (ASIL C)

Allocated to:

Contributes to: G002

Page	Date	Classification: CONFIDENTIAL	
52 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	

ID: SR636

[G] The BMS shall clear the cell undervoltage warning when the cell voltage rises above [XXX] V and remains stable for [XXX] time. (ASIL C)

Allocated to:

Contributes to: G002

ID: SR780

[X] CAN lines must be protected against spikes of upto xxx (ASIL B)

Allocated to:

Contributes to:

Page	Date	Classification: CONFIDENTIAL	
53 / 53	09-Jul-2025 1:47 pm	GENERATED DOCUMENT --- DO NOT EDIT!	